Organization Name

PCI Policy & Operating Procedures

Department Name:
Business Process Owner Name & Title:
Last Reviewed Date:

Purpose

The purpose of this document is to establish operational business processes and procedures for accepting and handling payment cards at {Organization name} as established by the Payment Card Industry Data Security Standards (PCI DSS) and in accordance with the NAME OF POLICY. In order to maintain compliance with PCI DSS, it is essential that departments that store, process, or transmit cardholder data adhere to procedures within the organization and departmental policies to help ensure the safe handling of cardholder data.

The collection and processing of card payments will be conducted in compliance with standards established by the Payment Card Industry Security Standards Council (PCI SSC), {Organization Name} policies, and the procedures outlined in this document. Departments are responsible for ensuring all processes, procedures, and technologies follow the security standards dictated by the PCI DSS and as approved by ITS and the PCI Data Security Standard team referenced in the Payment Card Policy This procedure document is reviewed on an annual basis to ensure operational processes are documented, up to date and known to all affected parties.

Business Process - Accepting and Handling Card Payments

User Access: Access to systems or equipment involved in storing, processing, or transmitting payment card data is restricted to only those individuals whose jobs require such access. Access is granted upon successful completion of all applicable training. When a user is terminated, transferred, or the job function no longer requires access, it is the merchant's responsibility to communicate such changes. To grant, modify, or revoke privileges, contact [help desk or other contact instructions].

Annual Awareness Training: All users authorized to process payments, handle payment cards, or work with payment card data will complete the annual PCI DSS awareness training. The PCI DSS training is intended to promote employee awareness of technical and operational requirements to protect payment card data. Upon hire, the merchant's business process owner must notify Training Coordinator of any new staff required to complete training.

Payment Card Terminals: Purchase or rental of payment card terminals, including mobile applications, must be coordinated through ITS and the PCI Data Security Standard team – only devices and locations that have been approved and tracked by the PCI Team may be used in any way associated with payment card processing. All devices must meet PCI DSS standards and BGSU policies. The merchant is responsible to ensure that only authorized staff have access to the terminal and are properly trained. Terminals must be inventoried with Director of Business Operations and must be maintained in a secure location. Sharing or transfer of wireless/mobile terminals between departments is not allowed without proper approval from Director of Business Operations.

Physical Device Security: Devices that capture payment card data via direct physical interaction with payment cards must be physically secured and protected from tampering and substitution. These devices include payment card terminals, card readers, and POS systems. Merchant is responsible for conducting inspections at the start of each day (prior to use), and completing the Device Inspection Log for all applicable devices. [include access instructions to this document.]

To conduct inspections, perform the following steps:

1. Compare the serial number and model number listed on the terminal to that included on the Device Inspection Log.
2. Review the tamper evident stickers on the surface of the terminal and make sure they are intact.
3. Inspect the terminal and review for foreign objects (e.g., skimmers), unexpected attachments or cables plugged into the device, pry marks, broken or stressed seams.
4. If you notice anything unusual or suspect that the terminal has been tampered with or substituted, follow the steps under Incident Response Procedures below.

When mobile terminals change hands between department users, an additional tamper check should be performed by the responsible party upon return.

Merchants should also ensure that employees are vigilant in preventing unauthorized access to devices that interact physically with payment cards. This includes the following measures:

1. Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.
2. Be aware of suspicious behavior. For example, attempts by unknown persons to unplug or open devices.
3. Do not alter or attempt to troubleshoot terminals. Troubleshooting support is provided by Financial Services.

Equipment & Use Overview:

Physical Equipment:

Equipment Type	Equipment Name	Terminal ID	Serial Number	Location/Physical Security	Purpose of Use

Ecommerce/outsourced/other usage:

For merchant ID ending:
Purpose of use:

Payment Card Processing Procedures:

1) **In Person – Merchant accepts credit card payment in person at xxx office. (If you do not accept card payments via in person, remove this portion of the procedures)**
   a) Request card from cardholder for processing. Ensure card is signed, if not, request ID.
   b) Process transaction via payment terminal.
   c) Have customer sign merchant copy/receipt. Verify signature matches back of card. Ask for photo ID from any customer without a signature on back of card.
   d) Give card and receipt to customer.

2) **Mail Order – Merchant receives mail orders for xxx and credit card information is returned on the form. (If you do not accept card payments via mail, remove this portion of the procedures)**
   a) Process mail orders via payment terminal
   b) Shred mailed in form containing CHD with a cross-cut or micro-cut shredder immediately upon processing transaction.
   c) If mail has been opened but unable to process immediately, check with your {APPROVAL BODY/PCI TEAM} about storage requirements.

3) **Phone Order – Merchant will accept credit card orders via phone only to XXX (number) and XXX (position). (If you do not accept card payments via phone, remove this portion of the procedures)**
   a) Credit card information will be taken and entered directly into credit card swipe terminal. No numbers or information will be written down.
   b) Confirmation Number will be given to customer once card is accepted.

4) **Fax is not considered a secure method for transmitting cardholder data and will not be accepted as a method of data receipt.**

5) **Email Order - BGSU does not accept credit card numbers sent in via email.**
   a) The credit card payment will NOT be processed.
   b) If numbers are received via email a response will be sent to the customer. The response will be a separate email – not a response to the original email, indicating the policy and procedure for sending credit card information.
   c) The email will be permanently deleted from email in box and trash.

6) **Online Orders**
   a) Online transactions are accepted via the Department's online solution SYSTEM at xxx (link).
   b) All transactions are conducted by the customer using customer personal devices; merchant employees do not enter transactions on behalf of customers.
   c) Individuals with authorized access to SYSTEM will fulfill orders on a daily basis.

End of Day Procedures/Batch Settlement: Terminals must be settled no less frequently than daily. It may be prudent, depending on the level of activity, to settle batches on a more frequent basis. The department must maintain all signed receipts and settlement reports in accordance with BGSU's Data Retention Policy.

[Provide any additional settlement details/end of day process here]

Disputes and Chargeback: Financial Services will receive and report chargebacks and transaction disputes to the merchant. Merchant can either accept or reject the chargeback. If rejected, the department will provide supporting documentation to justify that the transaction is valid that addresses the dispute reason. Failure to respond within the allocated timeframe will result in a financial loss to the department. Prompt attention to these matters is a priority. It is the department's responsibility to develop appropriate internal controls to mitigate risks related to chargebacks.

Refunds: Clear disclosure of return, refund, and cancellation policies can help to prevent potential cardholder disputes/chargebacks. Visa/MasterCard will support refund policies provided they are clearly disclosed to cardholders. Departments using SYSTEM must communicate refund/return/cancellation policy either in the sequence of pages before final checkout with a click to accept button or checkbox on the checkout screen / location with electronic signature.

1. The department's refund policy is xxxxxx

2. Procedures to refund a credit card transaction are included in the user manual for the POS devices and SYSTEM.

Incident Response Procedures: Merchant is responsible for reporting any suspected or confirmed security event where the confidentiality or integrity of payment card data (hard copy or electronic) may be impacted. This includes situations where payment card data may have been publicly viewable, or is discovered in an unexpected location, regardless of whether there is evidence of unauthorized access. In the event of such a suspected or confirmed incident:

1. Call 419-372-0999
2. Stop processing payments immediately.
3. Do not access or alter compromised systems.
4. Do not turn off the compromised machine.
5. Await further instructions from Incident Response Team.